Department of
INFORMATION
TECHNOLOGY

Maryland Contingency Planning Policy

Last Updated: 06/02/2017

Contents

1.0 Purpose

The Executive Branch agencies offer many important services to Maryland residents, employees, and partners. Efficient and effective contingency planning and disaster recovery creates resilient agencies that can continue essential operations in the event of unplanned service-interrupting events.

The Maryland Department of Information Technology (DoIT) is responsible for, and committed to, managing the confidentiality, integrity, and availability of State government information technology (IT) networks, systems, and applications within the scope of its authority. This includes ensuring that agencies proactively prepare for service interruptions and establish alternative methods to deliver essential functions.

This policy contains the requirements for Contingency Planning and Disaster Recovery capabilities within DoIT and other Maryland Executive Branch agencies in accordance with NIST Special Publication (SP) 800-53R4 and 800-34R1.

2.0 Document and Review History

This policy supersedes the Maryland Information Security Policy v3.1 (2013) Section 6.2: Contingency Planning and any policy regarding contingency planning declared prior to the 2017 Cybersecurity Program Policy. This document will be reviewed annually and is subject to revision.

Date	Version	Policy Updates	Approved By:
01/31/2017	v1.0	Approval of Draft	Maryland CISO
06/02/2017	v1.1	Initial Publication	Maryland CISO

3.0 Applicability and Audience

All Maryland Executive Branch agencies will comply with this policy and coordinate with the State CISO to obtain approval of agency contingency plans and associated disaster recovery documentation.

Maryland Department of Information Technology will be responsible for providing technical capabilities as services to Enterprise onboarded agencies in accordance with the requirements of this policy. Each agency is responsible for developing its individual contingency plan and documenting its disaster recovery processes to handle any interruption of service while abiding by any applicable law, regulation, standard, or contractual obligations establishing uptime requirements.

4.0 Policy

Maryland Executive Branch Agencies are considered **data owners** and each is required to create and manage a contingency plan and disaster recovery capability. DoIT Enterprise onboarded agencies will establish a contingency plan in accordance with this policy and may utilize technical services provided by DoIT to augment the recovery of systems and restoration of operational services. Agencies under the policy authority but not under direct management of DoIT must have a contingency plan and associated disaster recovery processes in accordance with this policy that include any technical capability required to ensure continuity of service or restoration of operation after a service-interrupting incident.

To manage the various technical and cyber security requirements for agencies onboarded into the DoIT Enterprise, DoIT will designate an **Information System Contingency Plan Coordinator (ISCP Coordinator)** to develop and manage the Enterprise cybersecurity contingency plan and work with Enterprise agencies to help them develop their individual plans. This role will be required to coordinate with agency managers and has authority to direct actions during a contingency operation. This role will have oversight for the engagement of this policy within the Enterprise.

NOTE: This policy focuses on cybersecurity contingency planning and disaster recovery. It is important for agencies to prepare an all-hazards contingency plan that considers and accounts for other potentially impacting events such as those posed by, but not limited to, environmental threats and workplace accidents.

4.1 Contingency Plan General Requirements

Agencies must develop a **contingency plan** for information systems that meets the requirements outlined below and accounts for the asset classification of each system in accordance with Federal Information Processing Standard Publication 199 (**FIPS 199)**.

#	Name	Requirement
A	Appoint ISCP Coordinator	The DoIT Enterprise and each non-Enterprise agency must appoint an Information System Contingency Plan Coordinator (ISCP Coordinator) who is responsible for continuity planning. Primary responsibilities include: ▪ Documenting contingency plans and disaster recovery processes for critical operation units ▪ Training employees responsible for execution of the contingency plan ▪ Managing disaster recovery related processes
B	Essential Mission and Function	Identifies essential missions and business functions and associated contingency requirements. This is usually done through a business impact analysis (BIA); see section 4.3 for additional guidance. NOTE: The FIPS 199 category for the availability security objective serves as a basis for the classification of assets in contingency planning.
C	Recovery Objectives and Timeliness	Provides recovery objectives, restoration priorities, and metrics for gauging compliance ▪ Defines recovery times and recovery points
D	Identify Roles	Defines contingency roles, responsibilities, and assigned individuals with contact information.
E	Focus on Essential Mission Continuity	Provides for maintaining essential missions and business functions despite an information system disruption, compromise, or failure.

#	Name	Requirement
F	Focus on System Restoration	Provides for eventual, full information system restoration without deterioration of the security safeguards originally planned and implemented.
G	Contingency Plan Approval	Contingency plans must be reviewed and approved by: ▪ State CISO or delegated authority (if Enterprise onboarded agency) ▪ Agency Deputy CIO or delegated authority (if IT is not actively managed by DoIT)
H	Distribute Plan	Distribute hard and soft copies of contingency plan to the following personnel: ▪ Executive leadership of the Agency (including State CISO if IT is managed by DoIT) ▪ Security and IT personnel involved in the implementation ▪ DoIT Security Operations Center (SOC)
I	Coordinate with Incident Handling	Coordinate contingency plan activities with incident handling activities.
J	Review Periodically	Review the contingency plan for each information system at least bi-annually (every other year) or when there are significant changes to the organization, information system, or operational environment.
K	Update Periodically	Update the contingency plan to incorporate changes to the organization, information system, operational environment, or to resolve problems encountered during contingency plan implementation, execution, or testing.
L	Notify Stakeholders of Changes	Communicate contingency plan changes to relevant system owners and stakeholders.
M	Safely Store Contingency Plan	Protect the contingency plan from unauthorized disclosure or modification. ▪ Contingency Plans are considered confidential information and should only be disclosed to those individuals with a need-to-know.

NOTE: DoIT and other agencies can follow guidance provided within NIST SP 800-34R1 “Contingency Planning Guide for Federal Information Systems” to formulate their contingency plans. This Special Publication has a series of examples and appendices that provide sample Information System Contingency Plan templates and Business Impact Analysis templates.

4.2 Additional Requirements

Agencies must meet the additional contingency plan requirements outlined below.

#	Name	Requirement
A	Contingency Training	Train personnel in their respective contingency roles and responsibilities; training must be provided: ▪ Annually ▪ Upon any significant changes to a system or the contingency plan itself

#	Name	Requirement
B	Contingency Plan Testing and Exercises	▪ Test the contingency plan for the IT asset by conducting annual exercises to determine the plan's effectiveness and the organization's readiness to execute the plan ▪ Review contingency test results and implement corrective actions where necessary
C	Alternate Storage Site	Establish an alternate storage site: ▪ Include necessary agreements to permit the storage and retrieval of information system backup information ▪ Ensure that the alternate storage site provides information security safeguards equivalent to that of the primary site NOTE: This requirement only applies to Moderate and High Asset Classifications under FIPS 199.
D	Alternate Processing Site	Establish an alternate processing site: ▪ Define recovery times and recovery points in the contingency plan ▪ Include necessary agreements to permit the resumption of information processing for essential mission and business functions within defined recovery times and recovery points when the primary processing capabilities are unavailable ▪ Ensure that equipment and supplies required to transfer and resume operations are available at the alternate processing site or contracts are in place to support delivery to the site within the organization-defined period for transfer and resumption ▪ Ensure that the alternate processing site provides information security safeguards equivalent to that of the primary site NOTE: This requirement only applies to Moderate and High Asset Classifications under FIPS 199.
E	Telecommunication Services	Establish alternate telecommunications services: Include agreements to permit the resumption of telecommunication services for essential missions and business functions within defined recovery times when the primary telecommunications capabilities are unavailable at either the primary or alternate processing or storage sites. NOTE: This requirement only applies to Moderate and High Asset Classifications under FIPS 199.

#	Name	Requirement
F	Information System Back-ups	▪ Make backups of the following information contained in information systems: ◆ User-level information ◆ System-level information ◆ Information system documentation, including security related documentation ▪ Ensure backups are created routinely to minimize the time to recover data and to recover the most recent data possible ▪ Routinely test the backups to ensure data is recoverable as expected ▪ Protect the confidentiality, integrity, and availability of backup information at storage locations as appropriate to the highest level of data categorization applicable
G	Information System Recovery and Reconstitution	Provide for the recovery and reconstitution of the information asset(s) to a known state after a disruption, compromise, or failure.

4.3 Business Impact Assessment

Conducting a business impact assessment (BIA) is an important step in implementing the contingency planning controls within NIST 800-53R4. Per NIST, the BIA enables the ISCP Coordinator to characterize system components and supported mission and business processes and to identify interdependencies. The purpose of the BIA is to correlate systems with critical mission and business processes and services, and based on that information, estimate the consequences of a disruption. The results of the BIA can guide the ISCP Coordinator in determining contingency requirements and priorities.

There are three steps to conducting a BIA:

1) Determine critical mission and business processes and recovery requirements;
2) Identify resource requirements; and
3) Identify recovery requirements for system resources.

4.4 Disaster Recovery

A Disaster Recovery Plan (DRP) is the process-based outcome of contingency planning. A DRP is an information system-focused plan designed to restore operability of the target system, application, or computer facility infrastructure after an emergency. Disaster recovery is the process by which an agency resumes (IT) business after a disruptive event, including specific steps that an agency and its employees must take to recover.

A disaster recovery plan must meet the minimum requirements outlined below.

#	Name	Requirement
A	Activation Criteria	Documents decision criteria used to activate the plan. Activation should occur when an assessment indicates that specified criteria are met.
B	Step by Step Procedure	Contains sequential step-by-step instructions to logically restore system components consistent with priorities identified in the BIA.

#	Name	Requirement
C	Identify Resources	Identifies who is responsible for which actions and documents coordination of activities if necessary.
D	Vendor and Contact Information	Contains vendor support and resource information, including multiple forms of contact information for vendor personnel.
E	Deactivation	Includes procedures for formally deactivating the DRP, including: ▪ Shutting down operations at alternative sites ▪ Retrieving pertinent materials, equipment, and back up media

5.0 Exemptions

This policy is established for use within the DoIT Enterprise. If an exemption from this policy is required, an agency needs to submit a DoIT Policy Exemption Form and clearly articulate the reason for the exemption. An operational risk assessment will be conducted to identify the risks and the agency's mitigation strategy associated with this exemption. If the agency can accept the risk, an exemption to this policy may be granted.

6.0 Policy Mandate and References

The Cybersecurity Program Policy mandates this policy. Related policies and resources include:

- Asset Management Policy
- Auditing and Compliance Policy
- Cybersecurity Assessment Policy
- Cybersecurity Incident Response Policy
- NIST SP 800-34R1 "Contingency Planning Guide for Federal Information Systems"

7.0 Definitions

Term	Definition
Contingency Plan	Management policy and procedures used to guide an enterprise response to a perceived loss of mission capability. The Contingency Plan is the first plan used by the enterprise risk managers to determine what happened, why, and what to do. It may point to the **Continuity of Operations Plan (COOP)** or Disaster Recovery Plan for major disruptions.
COOP Plan	A predetermined set of instructions or procedures that describe how an organization's mission-essential functions will be sustained within 12 hours and for up to 30 days as a result of a disaster event before returning to normal operations (NIST 800-34R1).
Disaster Recovery Plan	A written plan for recovering one or more information systems at an alternate facility in response to a major hardware or software failure or destruction of facilities. Disaster Recovery plan is used when the enterprise must recover (at its original facilities) from a loss of capability over a period of hours or days.
FIPS 199	A United States Federal Government standard that establishes security categories of information systems used by the Federal Government. FIPS 199 requires Federal agencies to assess their information systems in each of the categories of confidentiality, integrity and availability, rating each system as low, moderate or high impact in each category. The

Term	Definition
	most severe rating from any category becomes the information system's overall security categorization. For further guidance, see the official text of FIPS 199: http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.199.pdf
Information System Contingency Plan Coordinator (ISCP Coordinator)	May also be known as the COOP Coordinator in certain organizations. Individual who manages the policy and procedures designed to maintain or restore business operations, including computer operations, possibly at an alternate location, in the event of emergencies, system failures, or disasters.

8.0 Enforcement

The Maryland Department of Information Technology is responsible for enforcing policies for Enterprise onboarded agencies. The DoIT Cybersecurity Program identifies the minimum requirements necessary to comply with the information security standards and guidelines provided within Cyber Security Program Policy and its supporting policies. Agencies not directly managed by DoIT must exercise due diligence and due care to comply with the minimum standards identified by the relevant DoIT policies.

If DoIT determines that an agency is not compliant with this policy or any supporting policy, the non-compliant agency will be given a sixty (60) day notice to become compliant or at least provide DoIT a detailed plan to meet compliance within a reasonable time before the issue is reported to the Secretary of Information Technology. After which, the Secretary of Information Technology, or a designated authority, may extend a non-compliant agency’s window of resolution or authorize a DoIT representative to limit or restrict an agency’s access to external and internal communications (effectively shutting down connectivity) until such time that the agency becomes compliant.